

EXHIBIT 29

How Chrome Incognito keeps your browsing private

Incognito mode can help keep your browsing private from other people who use your device.

How Incognito mode works

When you first open a new Incognito window, you're creating a new Incognito browsing session. Any Incognito windows you open after that are part of the same session. You can end that Incognito session by closing all open Incognito windows.

In Incognito, none of your browsing history, [cookies](#) and site data, or information entered in forms are saved on your device. This means your activity doesn't show up in your Chrome browser history, so people who also use your device won't see your activity. Websites see you as a new user and won't know who you are, as long as you don't sign in.

If you're browsing in Chrome Incognito mode, you are, by default, not signed into any accounts or sites.

Your school, Internet Service Provider, or any parental tracking software may be able to see your activity. You can [check if your Chrome browser is managed](#).

You can choose to block third-party cookies when you open a new incognito window. [Learn more about cookies](#).

How Incognito mode protects your privacy

What Incognito mode does

- Browsing in Incognito mode means your activity data isn't saved on your device, or to a Google Account you're not signed into.
 - For example, you may use Incognito mode to shop online for a birthday gift for a family member who shares your device. If you don't sign in to your Google account, your shopping activity will not appear in your Chrome browsing activity and won't be saved to your Google Account.
- Each time you close all Incognito windows, Chrome discards any site data and cookies associated with that browsing session.
- Chrome doesn't tell websites, including Google, when you're browsing privately in Incognito mode.

What Incognito mode doesn't do

- Prevent you from telling a website who you are. If you sign in to any website in Incognito mode, that site will know that you're the one browsing and can keep track of your activities from that moment on.
- Prevent your activity or location from being visible to the websites you visit, your school, employer, or your Internet Service provider.
- Prevent the websites you visit from serving ads based on your activity during an Incognito session. After you close all Incognito windows, websites won't be able to serve ads to you based on your signed-out activity during that closed session.

You're in control

- Close all Incognito windows and tabs when you're done browsing. You end a session when you close all Incognito windows, so closing a single tab won't discard your data. If you see a number next to the Incognito icon on your desktop or at the bottom of your browser on a mobile device, you have more than one Incognito window or tab open.
- You can choose to sign in to any account when in Incognito mode. If you sign into a Google service, like Gmail, or a site, that site may remember your activity.
- Delete any downloads and bookmarks you don't want your device to remember. Files you download and bookmarks you create are saved in any mode.

[Learn more about using Incognito mode.](#)

EXHIBIT 30

Search & browse privately

You're in control of what information you share with Google when you search. To browse the web privately, you can use private browsing, sign out of your account, change your custom results settings, or delete past activity.

If you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari).

How private browsing works

Private browsing works differently depending on which browser you use. Browsing in private usually means:

- The searches you do or sites you visit won't be saved to your device or browsing history.
- Files you download or bookmarks you create might be kept on your device.
- Cookies are deleted after you close your private browsing window or tab.
- You might see search results and suggestions based on your location or other searches you've done during your current browsing session.

Important: If you sign in to your Google Account to use a web service like Gmail, your searches and browsing activity might be saved to your account.

Open private browsing mode

Learn how to search privately on these browsers:

- [Chrome](#)
- [Safari](#)
- [Microsoft Edge](#)
- [Firefox](#)

[Computer](#)

[Android](#)

[iPhone & iPad](#)

Sign out of your Google Account

When you browse in private you're signed out of your Google Account by default. If you sign in to your Google Account, through a web service like Gmail, your browsing activity might be saved to your account.

1. Visit any Google page, like google.com.
2. At the top right, click your Google Account profile picture > **Sign out**.
 - If you see the "Sign in" button, you're already signed out of your account.

Need more help?

Try these next steps:

Ask the Help Community

Get answers from community experts

EXHIBIT 31

Google is experimenting with new ways of supporting the delivery and measurement of digital advertising in ways that better protect people's privacy online via Chrome's [Privacy Sandbox](#) initiative. Users that participate in Chrome's Privacy Sandbox Origin Trials may see relevant ads from Google based on [Topics](#) or [FLEDGE](#) data stored on, or shared with, their browser. Google may also measure ad performance using [Attribution Reporting](#) data stored on, or shared with, their browsers. [More information on the Privacy Sandbox](#).

HOW GOOGLE USES INFORMATION FROM SITES OR APPS THAT USE OUR SERVICES

Many websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google.

For example, when you visit a website that uses advertising services like AdSense, including analytics tools like Google Analytics, or embeds video content from YouTube, your web browser automatically sends certain information to Google. This includes the URL of the page you're visiting and your IP address. We may also [set cookies on your browser](#) or read cookies that are already there. Apps that use Google advertising services also share information with Google, such as the name of the app and a unique identifier for advertising.

Google uses the information shared by sites and apps to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners' sites and apps. See our [Privacy Policy](#) to learn more about how we process data for each of these purposes and our [Advertising](#) page for more about Google ads, how your information is used in the context of advertising, and how long Google stores this information.

Our [Privacy Policy](#) explains the legal grounds Google relies upon to process your information — for example, we may process your information with your consent or to pursue legitimate interests such as providing, maintaining and improving our services to meet the needs of our users.

Sometimes, when processing information shared with us by sites and apps, those sites and apps will ask for your consent before allowing Google to process your information. For example, a banner may appear on a site asking for consent for Google to process the information that site collects. When that happens, we will respect the purposes described in the consent you give to the site or app, rather than the legal grounds described in the Google Privacy Policy. If you want to change or withdraw your consent, you should visit the site or app in question to do so.

Ad personalization

If ad personalization is turned on, Google will use your information to make your ads more useful for you. For example, a website that sells mountain bikes might use Google's ad services. After you visit that site, you could see an ad for mountain bikes on a different site that shows ads served by Google.

If ad personalization is off, Google will not collect or use your information to create an ad profile or personalize the ads Google shows to you. You will still see ads, but they may not be as useful. Ads may still be based on the topic of the website or app you're looking at, your current search terms, or on your general location, but not on your interests, search history, or browsing history. Your information can still be used for the other purposes mentioned above, such as to measure the effectiveness of advertising and protect against fraud and abuse.

When you interact with a website or app that uses Google services, you may be asked to choose whether you want to see personalized ads from ad providers, including Google. Regardless of your choice, Google will not personalize the ads you see if your ad personalization setting is off or your account is ineligible for personalized ads.

You can see and control what information we use to show you ads by visiting your [ad settings](#).

How you can control the information collected by Google on these sites and apps

Here are some of the ways you can control the information that is shared by your device when you visit or interact with sites and apps that use Google services:

- [Ad Settings](#) helps you control ads you see on Google services (such as Google Search or YouTube), or on non-Google websites and apps that use Google ad services. You can also [learn how](#) ads are personalized, opt out of ad personalization, and block specific advertisers.
- If you are signed in to your Google Account, and depending on your Account settings, [My Activity](#) allows you to review and control data that's created when you use Google services, including the information we collect from the sites and apps you have visited. You can browse by date and by topic, and delete part or all of your activity.
- Many websites and apps use Google Analytics to understand how visitors engage with their sites or apps. If you don't want Analytics to be used in your browser, you can [install the Google Analytics browser add-on](#). Learn more about [Google Analytics and privacy](#).
- [Incognito mode in Chrome](#) allows you to browse the web without recording webpages and files in your browser or Account history (unless you choose to sign in). Cookies are deleted after you've closed all of your incognito windows and tabs,

and your bookmarks and settings are stored until you delete them. Learn more about [cookies](#).

- Many browsers, including Chrome, allow you to block third-party cookies. You can also clear any existing cookies from within your browser. Learn more about [managing cookies in Chrome](#).

EXHIBIT 32

Privacy Disclosures Policy

When you use Google Analytics on your site or application, you must disclose the use of Google Analytics and how it collects and processes data.

For more information, see:

- [Google's Privacy & Terms](#)
- [Safeguarding your data](#)

Need more help?

Try these next steps:

Ask the Help Community

Get answers from community experts

EXHIBIT 33

Google Publisher Policies

(March 23, 2022) Due to the war in Ukraine, we will pause monetization of content that exploits, dismisses, or condones the war.

(March 10, 2022) Given the recent suspension of Google advertising systems in Russia, we'll be pausing the creation of new Russian accounts on AdSense, AdMob, and Google Ad Manager. Additionally, we will pause ads on Google properties and networks globally for advertisers based in Russia.

(March 3, 2022) Due to the ongoing war in Ukraine, we will be temporarily pausing ads from serving to users located in Russia.

(February 26, 2022) In light of the war in Ukraine, we are pausing Google's monetization of Russian Federation state-funded media.

We will continue to actively monitor the situation and make adjustments as necessary.

We are in the process of migrating and consolidating all of the Google Publisher Policies and Google Publisher Restrictions to the new [Publisher Policies Help Center](#). For now, you can still view all the policies in the [AdMob](#), [AdSense](#), and [Ad Manager](#) Help Centers, as well as the new Help Center.

When you monetize your content with Google ad code you are required to adhere to the following policies. Failure to comply with these policies may result in Google blocking ads from appearing against your content, or suspending or terminating your account.

These policies apply in addition to any other policies governing your use of Google publisher products.

Google helps to enable a free and open web by helping publishers monetize their content and advertisers reach prospective customers with useful, relevant products and services. Maintaining trust in the ads ecosystem requires setting limits on what we will monetize.

Google Publisher Policies are organized into the following categories:

- [Content policies](#)
- [Behavioral policies](#)
- [Privacy-related policies](#)
- [Requirements and other standards](#)

Learn more about the commonly used policy terms and what they mean in the [glossary](#).

Content policies

Illegal content

We do not allow content that:

- is illegal, promotes illegal activity, or infringes on the legal rights of others.

 [Learn more about illegal content](#)

Intellectual property abuse

We do not allow content that:

- infringes copyright. It is our policy to respond to notices of alleged infringement that comply with the Digital Millennium Copyright Act (DMCA). You can file a counter-notification via [this form](#).
- sells or promotes the sale of counterfeit products. Counterfeit goods contain a trademark or logo that is identical to or substantially indistinguishable from the trademark of another. They mimic the brand features of the product in an attempt to pass themselves off as a genuine product of the brand owner.

 [Learn more about intellectual property abuse](#)

Dangerous or derogatory content

We do not allow content that:

- incites hatred against, promotes discrimination of, or disparages an individual or group on the basis of their race or ethnic origin, religion, disability, age, nationality, veteran status, sexual orientation, gender, gender identity, or other characteristic that is associated with systemic discrimination or marginalization.
Examples: Promoting hate groups or hate group paraphernalia, encouraging others to believe that a person or group is inhuman, inferior, or worthy of being hated
- harasses, intimidates, or bullies an individual or group of individuals.
Examples: Singling out someone for abuse or harassment, suggesting a tragic event did not happen or that victims or their families are actors or complicit in a cover-up of the event
- threatens or advocates for physical or mental harm to oneself or others.
Examples: Content advocating suicide, anorexia, or other self-harm; threatening someone with real-life harm or calling for the attack of another person; promoting, glorifying, or condoning violence against others; content made by or in support of terrorist groups or transnational drug trafficking organizations, or content that promotes terrorist acts, including recruitment, or that celebrates attacks by transnational drug trafficking or terrorist organizations
- exploits others through extortion.
Examples: Exploitative removals, revenge porn, blackmail

[!\[\]\(d3fb9f94af8b26d1c844efa9a98805b0_img.jpg\) Learn more about dangerous and derogatory content](#)

Animal cruelty

We do not allow content that:

- promotes cruelty or gratuitous violence towards animals.
Examples: Promoting animal cruelty for entertainment purposes, such as cock or dog fighting
- promotes the sale of products obtained from endangered or threatened species.
Examples: Sale of tigers, shark fins, elephant ivory, tiger skins, rhino horn, dolphin oil

[!\[\]\(e1d6102fe77919492c04879c8450f1f5_img.jpg\) Learn more about animal cruelty](#)

Misrepresentative content

Misleading representation

We do not allow content that:

- misrepresents, misstates, or conceals information about the publisher, the content creator, the purpose of the content, or the content itself.
- falsely implies having an affiliation with, or endorsement by, another individual, organization, product, or service.
Examples: Impersonating Google products, misusing company logos

[!\[\]\(104fbf564e2e5a8fbd84f31656d114c7_img.jpg\) Learn more about misleading representation](#)

Unreliable and harmful claims

We do not allow content that:

- makes claims that are demonstrably false and could significantly undermine participation or trust in an electoral or democratic process.
Examples: information about public voting procedures, political candidate eligibility based on age or birthplace, election results, or census participation that contradicts official government records
- promotes harmful health claims, or relates to a current, major health crisis and contradicts authoritative scientific consensus.
Examples: Anti-vaccine advocacy, denial of the existence of medical conditions such as AIDS or Covid-19, gay conversion therapy

- contradicts authoritative scientific consensus on climate change.

[!\[\]\(d84e7ea36f695d92cb39ec32c307ac93_img.jpg\) Learn more about unreliable and harmful claims](#)

Deceptive practices

We do not allow:

- enticing users to engage with content under false or unclear pretenses.
- attempting to steal personal information or trick users into sharing personal information

Example: Social engineering like phishing

- promoting content, products, or services using false, dishonest, or deceptive claims.

Examples: "Get Rich Quick" schemes

- coordinating with other sites or accounts and concealing or misrepresenting your identity or other material details about yourself, where your content relates to politics, social issues or matters of public concern.
- directing content about politics, social issues, or matters of public concern to users in a country other than your own, if you misrepresent or conceal your country of origin or other material details about yourself.

[!\[\]\(d0262bbe9d2356661a2e89321dfcc781_img.jpg\) Learn more about deceptive practices](#)

Manipulated media

We do not allow content that:

- deceives users through manipulated media related to politics, social issues, or matters of public concern.

[!\[\]\(274fd520e03b61c1b9ffc861754cacdc_img.jpg\) Learn more about manipulated media](#)

Enabling dishonest behavior

We do not allow content that:

- helps users to mislead others.

Examples: Creating fake or false documents such as passports, diplomas, or accreditation; sale or distribution of term papers, paper-writing or exam-taking services; information or products for passing drug tests

- promotes any form of hacking or cracking and/or provides users with instructions, equipment, or software that tampers with or provides unauthorized access to devices, software, servers, or websites.

Examples: Pages or products that enable illegal access of cell phones and other communications or content delivery systems or devices; products or services that bypass copyright protection, including circumvention of digital rights management technologies; products that illegally descramble cable or satellite signals in order to get free services; pages that assist or enable users to download streaming videos if prohibited by the content provider

- enables a user, or promotes products and services that enable a user, to track or monitor another person or their activities without their authorization.

Examples: Spyware and technology used for intimate partner surveillance including but not limited to spyware/malware that enables a user to monitor another person's texts, phone calls, or browsing history; GPS trackers specifically marketed to spy or track someone without their consent; promotion of surveillance equipment (e.g. cameras, audio recorders, dash cams, nanny cams) marketed with the express purpose of spying

This does not include (a) private investigation services or (b) products or services designed for parents to track or monitor their underage children.

[!\[\]\(9cfd7b8995754ae2aef7ec59dba55501_img.jpg\) Learn more about enabling dishonest behavior](#)

Malicious or unwanted software

We do not allow content that:

- contains malicious software or "malware" that may harm or gain unauthorized access to a computer, device, or network.

Examples: Computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, rogue security software, and other malicious programs or apps

- violates [Google's Unwanted Software policy](#) .

Examples: Failure to be transparent about the functionality that the software provides or the full implications of installing the software; failing to include Terms of Service or an End User License Agreement; bundling software or applications without the user's knowledge; making system changes without the user's consent; making it difficult for users to disable or uninstall the software; failing to properly use publicly available Google APIs when interacting with Google services or products

[!\[\]\(96cc62f861fdd6e50510c0224a756dff_img.jpg\) Learn more about malicious or unwanted software](#)

Sexually explicit content

We do not allow content that:

- includes graphic sexual text, image, audio, video, or games.

Examples: Sex acts such as genital, anal, and/or oral sex; masturbation; cartoon porn or hentai; graphic nudity

- contains non-consensual sexual themes, whether simulated or real.

Examples: Rape, incest, bestiality, necrophilia, snuff, lolita or teen-themed pornography, underage dating

[!\[\]\(4688aadfd656ded00cd6bdfae55089a9_img.jpg\) Learn more about sexually explicit content](#)

Compensated sexual acts

We do not allow content that:

- may be interpreted as promoting a sexual act in exchange for compensation.

Examples: Prostitution; companionship and escort services; intimate massage; cuddling sites; compensated dating or sexual arrangements where one participant is expected to provide money, gifts, financial support, mentorship, or other valuable benefits to another participant such as "Sugar" dating

[!\[\]\(9db214d549b9aeebe72aa11d3a5c4b1a_img.jpg\) Learn more about compensated sexual acts](#)

Mail order brides

We do not allow content that:

- facilitates marriage to a foreigner.

Examples: Mail order brides, international marriage brokers, romance tours

[!\[\]\(fd47dc3c71882b0b4a62715dd757d994_img.jpg\) Learn more about mail order brides](#)

Adult themes in family content

We do not allow content that:

- is made to appear appropriate for a family audience, but contains adult themes including sex, violence, or other depictions of children or popular children's characters that are unsuitable for a general audience.

[!\[\]\(220899daa07e43db9eb76860c91c848f_img.jpg\) Learn more about adult themes in family content](#)

Child sexual abuse and exploitation

We do not allow content that:

- Sexually exploits or abuses children or content that promotes the sexual exploitation or abuse of children. This includes all child sexual abuse materials.
- Endangers children. Including but not limited to:

- 'Child grooming' (for example, befriending a child online to facilitate, either online or offline, sexual contact and/or exchanging sexual imagery with that child);
- 'Sextortion' (for example, threatening or blackmailing a child by using real or alleged access to a child's intimate images);
- Sexualization of a minor (for example, content that depicts, encourages or promotes the sexual abuse or exploitation of children); and
- Trafficking of a child (for example, advertising or solicitation of a child for commercial sexual exploitation).

We will take appropriate action, which may include reporting to the National Center for Missing & Exploited Children and disabling accounts. If you believe a child is in danger of or has been subject to abuse, exploitation, or trafficking, contact the police immediately. If you have concerns a child is being or was being endangered in connection with our products, you can [report the behavior to Google](#).

 [Learn more about child sexual abuse and exploitation](#)

Behavioral policies

Dishonest declarations

Information provided by publishers to enable their use of or interaction with Google advertising systems:

- must be materially accurate and complete, without misleading omissions; and
- cannot be expressed in a deceptive or misleading manner.

Examples: The personal information or payment details provided by a publisher are materially incomplete, obscured or inaccurate. Information provided about a publisher's website (e.g., in the ads.txt file) or app (e.g., in the app-ads.txt file) is inaccurate. Ad requests that contain partial or inaccurate URLs or AppIDs.

 [Learn more about dishonest declarations](#)

Ads interfering

Google-served ads interfering with content or user interactions

We do not allow Google-served ads that:

- overlay or are adjacent to navigational or other action items and may lead to unintended ad interactions,
- severely interfere with consumption of content including overlaying the content or pushing the content off the display,
- are placed on a "dead end" screen where the user is not able to exit the screen without clicking the ad.

 [Learn more about ads interfering](#)

Inventory value

Google-served ads on screens without publisher-content

We do not allow Google-served ads on screens:

- without publisher-content or with low-value content,
- that are under construction,
- that are used for alerts, navigation or other behavioral purposes

 [Learn more about Google-served ads on screens without publisher-content](#)

Out of context ads

We do not allow Google-served ads:

- in apps or web pages that run in the background,

- that appear outside the display,
- when the user's attention is expected to be elsewhere and not on the screen hosting the ad.

It must be clear to the user with which publisher-content the ad is associated.

 [Learn more about out of context ads](#)

Google-served ads on screens with replicated content

We do not allow Google-served ads on screens:

- with embedded or copied content from others without additional commentary, curation, or otherwise adding value to that content.

You are also required to comply with our [Intellectual property abuse policy](#).

 [Learn more about Google-served ads on screens with replicated content](#)

More ads or paid promotional material than publisher-content

We do not allow Google-served ads on screens:

- with more ads or other paid promotional material than publisher-content.

 [Learn more about More ads or paid promotional material than publisher-content](#)

Unsupported languages

We do not allow content that:

- is not primarily in one of the supported languages.

 [Learn more about unsupported languages](#)

Privacy-related policies

Privacy disclosures

Publishers must:

- have and abide by a privacy policy that clearly discloses any data collection, sharing and usage that takes place on any site, app, email publication or other property as a consequence of your use of Google products. The privacy policy must disclose to users that third parties may be placing and reading cookies on your users' browsers, or using web beacons to collect information as a result of ad serving on your website.

To comply with this disclosure obligation with respect to Google's use of data, you have the option to display a prominent link to [How Google uses data when you use our partners' sites or apps](#).

 [Learn more about privacy disclosures](#)

Cookies on Google domains

Publishers must:

- not set a cookie on Google's domains or modify, intercept or delete cookies set on Google's domains.

 [Learn more about cookies on Google domains](#)

Identifying users

Publishers must:

- not use device fingerprints or locally shared objects (e.g., Flash cookies, Browser Helper Objects, HTML5 local storage) other than HTTP cookies, or user-resettable mobile device identifiers

designed for use in advertising

- not pass any information to Google data that Google could use or recognize as personally identifiable information; or that permanently identifies a particular device (such as a mobile phone's unique device identifier if such an identifier cannot be reset).
- not use our services to identify users or facilitate the merging of personally identifiable information with information previously collected as non-personally identifiable information without robust notice of, and the user's prior affirmative (i.e., opt-in) consent to, that identification or merger. Irrespective of users' consent, you must not attempt to disaggregate data that Google reports in aggregate.

For more information, please refer to [Guidance for complying with the Identifying Users Policy](#).

- comply with the [EU user consent policy](#) .

 [Learn more about identifying users](#)

Use of device and location data

If publishers collect, process, or disclose information that identifies or can be used to infer an end user's precise geographic location, such as sourced from GPS, wifi or cell tower data then,

Publishers must:

- disclose to the user, via an interstitial or just-in-time notice, the purposes for which their data may be used (including, ad personalization, analytics, and attribution, as applicable), including that the data may be shared with partners;
- obtain express (i.e., opt-in) consent from end users before collecting, processing, or disclosing such information;
- send such information to Google in an encrypted state or via an encrypted channel; and
- disclose such information collection, processing, or disclosure in all applicable privacy policies.

 [Learn more about use of device and location data](#)

Standard Contractual Clauses (SCCs)

Google relies on Standard Contractual Clauses (SCCs) for transfers of online advertising and measurement personal data out of Europe. For those [services where Google acts as a processor](#) , the [Google Ads Data Processing Terms](#) include, as necessary for the relevant data transfers, both the relevant SCCs issued by the European Commission (to help legitimize data transfers under the GDPR) and UK SCCs (to help legitimize data transfers under the GDPR as incorporated into UK law). Similarly, for [those services where Google acts as a controller](#) , the [Google Ads Controller-Controller Data Protection Terms](#) include, as necessary for the relevant data transfers, both the relevant European Commission-issued SCCs and UK SCCs.

If partner processes personal data that originated in the European Economic Area, UK, or Switzerland and that is made available by Google in connection with partner's use of Google Ad Manager, then:

- partner must only use that personal data in a manner consistent with the consent provided by the data subject to whom it relates;
- partner must provide a level of protection for that personal data that is at least equivalent to that required under the SCCs; and
- if partner determines that it cannot comply with the above requirements, partner must notify Google in writing, and either cease processing the personal data or take reasonable and appropriate steps to remedy such non-compliance.

 [Learn more about Standard Contractual Clauses \(SCCs\)](#)

Children's Online Privacy Protection Act (COPPA)

If you implement any Google advertising service on a site or section of a site that is covered by the Children's Online Privacy Protection Act (COPPA), you must:

- notify Google of those sites or sections of sites covered by COPPA using the [Google Search Console](#) , tag the ad request using the [AdMob SDK](#) , or tag your site, app, or ad request for child-directed treatment;

- not use interest-based advertising (including remarketing) to target:
 - past or current activity by users known by you to be under the age of 13 years or
 - past or current activity on sites directed at users under the age of 13 years.

 [Learn more about Children's Online Privacy Protection Act \(COPPA\)](#)

Requirements and other standards

Webmaster Guidelines

You must not:

- place Google-served ads on screens that don't follow the [Webmaster Quality Guidelines](#) .

 [Learn more about Webmaster Guidelines](#)

Abusive experiences

You must not:

- place Google-served ads on screens that contain [abusive experiences](#) .

 [Learn more about abusive experiences](#)

Better Ads Standards

You must not:

- place Google-served ads on screens that do not conform to the [Better Ads Standards](#) . For more information about the types of disallowed ad experiences, please visit the [Coalition for Better Ads](#) website.

 [Learn more about Better Ads Standards](#)

Authorized inventory

You must not:

- place Google-served ads on a domain that uses [ads.txt](#) where you are not included as an authorized seller of the inventory in the [ads.txt](#) file.

For syndication partners, Parents must ensure Children promptly add an [ads.txt](#) file to Child domains with Parents as authorized sellers of Child Inventory.

 [Learn more about authorized inventory](#)

Sanctions compliance

Google must comply with sanctions and export controls maintained by the United States Treasury Department's [Office of Foreign Assets Control](#) (OFAC), United States Commerce Department's Bureau of Industry & Security and other applicable sanctions. As a result, Google publisher products are not available to publishers in the following countries or territories:

- Crimea
- Cuba
- So-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR)
- Iran
- North Korea
- Syria

Google publisher products also may not be used for or on behalf of a party located in the above listed sanctioned countries or regions.

In addition, Google publisher products are not eligible for any entities or individuals that are restricted under applicable trade sanctions and export compliance laws. Google publisher products are not

eligible for entities or individuals owned or controlled by or acting for or on behalf of such restricted entities or individuals.

Publishers must also comply with applicable sanctions and export regulations, which includes OFAC sanctions, and agree to not cause Google to violate these regulations. You cannot use Google publisher products for or on behalf of restricted entities or individuals. You cannot use Google publisher products for or on behalf of entities or individuals located in sanctioned countries or regions.

 [Learn more about sanctions compliance](#)

Need more help?

Try these next steps:

Ask the Help Community

Get answers from community experts

Contact us

Tell us more and we'll help you get there

EXHIBIT 34

Website Cookie Policy

Last Updated: August 31, 2020; Effective: September 1, 2020

This Cookie Policy describes the different types of cookies that may be applied on the equipment of consumers who visit granie3.com and any other websites (the "Sites") owned and operated by Drudge Report, Inc. and its affiliates (collectively, "Drudge Report").

We may update this Cookie Policy from time to time in order to reflect, for example, changes to the cookies we use or for other operational, legal or regulatory reasons. Please therefore re-visit this Cookie Policy regularly to stay informed about our use of cookies and similar technologies. The date at the top of this Cookie Policy indicates when it was last updated.

If you have any further queries, please contact us by email at drudge@drudgereport.com.

Some cookies that we use through the Sites will collect personal information about you, or information that becomes personal information if we combine it with other data. Any personal information that we collect will be used in accordance with our [Privacy Policy](#).

WHAT IS A COOKIE?

Cookies are a standard feature of websites that allow us to collect certain information from your browser or device when you visit our Sites. In relation to the use of cookies by our partners and clients, note that we do not have access or control over these cookies.

WHAT COOKIES DO WE USE?

We use a variety of cookies on the Drudge Report Sites for several reasons. We also may use web logs, pixel tags, or web beacons, which are pieces of code that may be used to read and place cookies on a web browser, to collect information about how you interact with websites or advertisements.

The sections below describe the types of cookies most frequently used by Drudge Report on the Sites and explain their use.

Essential Cookies

We use cookies that are essential to making the Sites work. These types of cookies enable you to move around the Sites and use their features. For example, we may use cookies to record a user login, manage user sessions, authenticate users of our management apps, or adjust settings and functionality on the Sites. Without these cookies, we may not be able to provide the services that are necessary for you to be able to use the Sites.

Cookie Names	Purpose
__cfduid	This cookie is used to identify individual clients behind a shared IP address and apply security settings on a per-client basis. For example, if a visitor is in a coffee shop where there may be several infected machines, but the specific visitor's machine is trusted (for example, because they completed a challenge within your Challenge Passage period), the cookie allows our security system to identify that client and not challenge them again. It does not correspond to any user ID in our web application, and does not store any personally identifiable information.
in_ca	This indicates you are in California, as inferred from your IP address. California residents are shown an alternate version of the Drudge Report including all required notices.
optout	This indicates you exercised your right to opt out of "sale" of your information.

Preference Cookies

We also use cookies that collect information about your choices and preferences. These cookies may allow us to remember language or other local settings and customize the Sites accordingly. For example, we use a cookie to confirm consent to use cookies.

Cookie Names	Purpose
consent	This indicates you consented to our privacy policy so it will no longer show you the consent banner.

Analytics Cookies

These cookies collect information about how people are using the Sites, for example which pages are visited the most often, how visitors move from one webpage to another, and whether visitors experience any difficulty using the Sites. Overall, these cookies provide us with analytical information about how the Sites are performing and how we can improve it, and in some instances, whether our advertising is effective or not.

Cookie Names	Purpose
Google Analytics [_ga.js]	<p>We use Google Analytics cookies to collect aggregate statistical data about how visitors use the Sites so that we can improve the user experience and serve up the content our visitors find most useful. Google Analytics cookies store information such as what pages users visit, how long they are on the Sites, how they arrived at the Sites, and what they click on.</p> <p>To learn more about Google's practices and to opt out, please visit http://www.google.com/policies/privacy/partners/, https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage, and https://tools.google.com/dlpage/gaoptout.</p> <p>The following cookies may be used in connection with Google Analytics:</p> <p>[_utma] Used to distinguish users and sessions.</p> <p>[_utmb] Used to determine new sessions/visits.</p> <p>[_utmc] Not used in ga.js. Set for interoperability with urchin.js. Historically, this cookie operated in conjunction with the __utmb cookie to determine whether the user was in a new session/visit.</p> <p>[_utmt] Used to throttle request rate (e.g., to reduce the frequency with which a browser may request data from the server).</p> <p>[_utmz] Stores the traffic source or indicates the advertising campaign that explains how the user reached our Sites.</p>
eproofui	This cookie is used to track the number of times you access the Drudge Report, at what times, and from where.

Advertising Cookies

We may partner with certain third parties to deliver advertising that we believe may interest you based on your activity on our Sites and other websites over time. These third parties may set and access cookies on your computer or other device and may also use web logs, pixel tags, or web beacons. These cookies are used to deliver advertisements that are more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as to help measure the effectiveness of the advertising campaign.

Cookie Names	Purpose
Advertising Partners [*]	These cookies are associated with one of our advertising partners. These are used for preference based advertising. To prevent sharing among these partners, California residents may opt-out .
Google Ads [_gads]	This is a cookie associated with Google Ads, a digital advertising service. To learn more about Google's practices and to opt out, please visit Ads Settings .
Quantcast [_qca]	This is a cookie associated with Quantcast, a digital advertising company. Quantcast provides website rankings, and the data the cookie collects is also used for audience segmentation and targeted advertising. To learn more about Quantcast's practices and to opt out, please visit https://www.quantcast.com/opt-out/ .

* A range of cookie names may be used occasionally, depending on your browsing activity. All cookies not explicitly named here are Advertising Cookies from Advertising Partners.

HOW DO I MANAGE COOKIES?

You have the right to decide whether to accept or reject cookies. In addition to the options provided above, you may refuse or accept cookies from the Sites at any time by activating settings on your browser. Information about the procedure to follow in order to enable or disable cookies can be found on your Internet browser provider's website via your help screen. You may wish to refer to <http://www.allaboutcookies.org/manage-cookies/index.html> for information on commonly used browsers. Please be aware that if cookies are disabled, some website features may not operate as intended. For example, you will be unable to dismiss our consent banner for repeated visits, and if you are a California resident, you may not be shown the California version of our web site.

EXHIBIT 35



Privacy and Cookie Policy

This Privacy Policy applies to the collection, use, and transmission of data of and about visitors to www.bsfllp.com and to other websites maintained by Boies Schiller Flexner LLP and/or Boies Schiller Flexner (UK) LLP (the "Firms") that link to this Privacy Policy.

Our Commitment to Your Privacy

Thank you for visiting the Firms' website. The Firms are committed to protecting and respecting the privacy of visitors to their websites. This Privacy Policy describes:

- how and why we collect certain information from you via the website and the online services provided through the website;
- with whom we share such information;
- how we store that information, including information as to how we secure the information;
- how you can access and update such information; and
- other relevant aspects of our policy.

If you have any questions regarding this Privacy Policy or our information collection and use practices, please contact us using the information in the "Contact Us" section below.

Information We Collect and How We Use It

Non-personal Information. Like many websites, we may collect certain technical information about your use of the website and generally this is not information the Firms could use to identify you without reference to other information. For example, we may collect your internet protocol (IP) address, browser type, the identity of your internet service provider (ISP), the number and duration of page visits, how you were directed to the website, and the number of clicks you make when you use the website. This does not include demographic information about you. We track and reference your usage information, in aggregation with the usage information of other visitors to the website, to better understand how effective our website is and how visitors interact with it. We may use third parties, such as Google and our website host, to

provide analytics services based on this data. The analytics and the underlying data are generally only accessible to the Firms and their third party providers.

In addition, some portions of our website may use session or persistent cookies. A cookie is a file that web servers place on an Internet user's computer. Cookies are designed to store basic information about the user and transmit that information back to servers that recognize them. They may be used to measure visitor behavior on and in connection with a website, including through the transmission of usage information. A session cookie stays on your machine only as long as your browser is open and tuned to the site that placed the cookie. A persistent cookie remains on your machine after you log out of your account and will become active again when you return to the website. Some portions of our website use cookies as described below. You may be able to change your Internet browser settings to reflect your preference for accepting, storing, and/or deleting cookies.

Please note, do not track signals are not effective on our website.

Personal Information

You have the opportunity to submit personal information (such as name, company affiliation, job title, email address, phone number, physical address, and whether or not you are a current firm client) via the website for the following purposes:

- **Receiving BSF communications or publications.** If you request an eNewsletter, a White Paper, or a subscription to either or a Blog, we use this information to send you the requested publications. The Firms or their service providers may use persistent cookies to identify you as a subscriber and continue to deliver content to you.
- **Registering as an alumnus.** If you choose to register as an alumnus of the firm, we use this information to send you news and updates.
- **Using the My Binder function.** If you choose to sign up to use the "My Binder" function on this website, we use this information to create and permit access to your My Binder account.
- **Asking for further information.** You have the opportunity to provide feedback to us or make inquiries of us through the "Contact Us" link. We use this information to communicate with you as requested.

Sharing of Your Information

We may share your personal information with third parties in one or more of the following ways:

- Third party service providers, such as website hosts: We use third parties to host our website. These third parties may have access to your personal information submitted through the website consistent with the hosting of the site.

- Third party organizations that otherwise assist the Firms in providing goods, services or information, including cloud storage providers in the case of firm and client data.
- Successor organizations. In the event the Firms undergo a business transition (such as a merger or acquisition), we may transfer your personal information to the successor organization in such transaction. If material changes to the Firms' privacy practices will occur as a result of the business transition, the Firms will post a notice on the website.
- Auditors and other professional advisers.
- Law enforcement or other government and regulatory agencies or other third parties as required by, and in accordance with, applicable law or regulation.

We do not share or sell personally identifiable information to third parties for their commercial marketing purposes.

We reserve the right to disclose your personal information as permitted or required by law or regulation.

The information which we may collect from you may be transferred to, stored and processed by us in a destination outside of the European Economic Area (the "EEA"), including the United States and countries whose laws concerning data privacy may not be comparable to those in EEA jurisdictions, but will only be done so in accordance with applicable laws.

How We Store Information Collected from You

We store your personal and non-personal information with the hosting providers and cloud storage providers discussed above. Our administrative departments may store application information in accordance with firm retention practices.

The Firms will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with our normal procedure, this policy, and all applicable laws.

The Firms use reasonable administrative, technical, and physical security measures to protect your personal and non-personal information, online and offline. Because of the nature of our website, we do not currently encrypt any transmissions to or from the website in any manner. If you are uncomfortable with the unencrypted transmission of personal information described herein, please do not submit information to us through the website.

Our employees, including contract employees, are generally subject to restrictions which limit their use of information obtained from the Firms to the business purpose of providing our services to you.

However, while we take reasonable precautions against possible security breaches of the website and our customer databases and records, no website or Internet transmission is completely secure,

and we cannot guarantee that unauthorized access, hacking, data loss, or other breaches will never occur. Owners of personal information are generally advised to take steps to keep their personal information safe to the extent possible.

How to Access and Update Your Personal Information

At any time, you may contact the Firms to request that we:

- provide you with a copy of any personal data pursuant to Article 15 of the EU General Data Protection Regulation (EU) 2016/679 (“GDPR”) and/or Section 45 of the Data Protection Act 2018 (“DPA”) (to the extent that each of the GDPR and DPA applies to you); and/or
- make changes to your personal information (including deleting such information).

If you request that the Firms update or otherwise modify your information, we will amend your personal information within a reasonable time after your request. To request modifications of personal information that the Firms possesses about you, please contact us using the information in the “Contact Us” section below.

However, please note that, after your personal information is changed, the Firms will continue to have the right to store all personal information collected from you through the website (including personal information which is no longer in active use due to its amendment in accordance with this Section) in our archives and to use and disclose such personal information for certain purposes permitted or required by applicable laws, including as we deem necessary to comply with any applicable law, regulation, legal process or governmental request, to enforce our rights, or to protect the safety and security of our website or other users. For example, we are required by law to retain certain job applicant information for a minimum of three years (although where the GDPR applies we may retain job applicant information for a more limited period of time).

Our Policies Concerning Information from Minors

This website is not intended for children under the age of thirteen and we do not knowingly collect personal information from such children. Children under the age of thirteen should not use our website or provide us with any personal information.

In the event that we learn that we have inadvertently gathered personal information from children under the age of 13, we will use reasonable efforts to erase such information from our records.

Changes to Our Privacy Policy

We reserve the right to modify or amend this Privacy Policy at any time. If such modification includes any significant, material changes, we will provide notice of the update on our website. You should

visit the website frequently to remain informed of this policy's current content.

Contact Us

The data controllers are Boies Schiller Flexner (UK) LLP and/or Boies Schiller Flexner LLP.

If you have any questions, comments or concerns regarding our Privacy Policy and/or practices relating to personal data, please send an Email to **privacy@bsfllp.com**.

This policy was last updated on April 29, 2020.

Copyright © 2022 Boies Schiller Flexner LLP.
All Rights Reserved.

Attorney Advertising.
Prior results do not guarantee a similar outcome.

LEGAL
PRIVACY AND COOKIE POLICY
LONDON LEGAL NOTICES

VISIT US ON LINKEDIN

EXHIBIT 36

The Fee Is Free, Only Pay If We Win. Contact Us Today.

X

MORGAN & MORGAN, P.A. PRIVACY POLICY

Morgan & Morgan, P.A. and its affiliates (referred to herein as “MM”, “we”, “us”, or “our”) respects your privacy and is committed to complying with this privacy policy (“Privacy Policy”), which describes what information we collect about you, how we use it, with whom we may share it, and what choices you have regarding our use of your information. This Privacy Policy applies to personal information collected in connection with our website located at <https://forthepeople.com> and any other webpage that MM maintains that links to this Privacy Policy (collectively, the “Site”), any current or future mobile applications associated with MM or the website (collectively, the “App”), our email communications, our social media pages, other online or wireless offerings that post a link to the Privacy Policy, and other circumstances in connection with the services we provide (collectively, the “Platform”).

TYPES OF PERSONAL INFORMATION WE COLLECT

The types of personal information we collect will depend on the services you request and, if you are a client, the nature of our representation or your case. The table below describes some of the categories (with non-exhaustive examples) of personal information we may collect about you:

--	--

Categories	Examples
A. Individual Identifiers and Demographic Information	Contact information , such as name, email address, phone number, mailing address, job title, and organization. Identifiers , such as client ID, username, IP address, device ID, and other online identifiers that may be collected automatically when you use the Platform. Demographic information , such as

Search...

[Locations](#)
[Practice Areas](#)
[Car Accidents](#)
[Attorneys](#)
[About](#)
[Our Results](#)
[Contact](#)
[En Español](#)

MORGAN & MORGAN

Call Now • Open 24/7
877 633 8213

Personal Information	invoices, and other payment or bank account details. Medical information , such as doctor's notes, treatment plans, medical conditions, prescription medicines, insurance documentation, doctor visit information, daily symptom reporting, and other records and information.
C. Geolocation Data	Precise physical location , which we may collect via the App if you consent to that collection through the App.
E. Sensory Data	Call recordings , such as our recordings of calls you make to our customer service team. Other sensory data , such as any audio recordings, photographs, videos, or similar data that may be provided as part of a case file.
F. Biometric Information	Biometric information , such as facial scans or fingerprint scans if you opt-in to using this information for logging in or authenticating your account on the

	App.
G. Commercial Information	<p>Representation information, such as details about your claim, case, or other legal matter, the distribution of settlement of other payments to you (if applicable).</p> <p>Account information, such as the username and password you provide when you register for an account and any information stored or transmitted in your account or profile.</p> <p>Communications, such as when you call or email us, confidential and privileged communications that you may make with our attorneys, and your conversations with our digital chat services.</p>
H. Internet or Network Activity	<p>Online activity information, such as linking pages, pages or screens viewed, time spent on a page or screen, navigation paths between pages or screens, information about activity on a page or screen, access times, duration of access, and other online activity information.</p> <p>Device information, such as computer and mobile operating system, operating system type and version number, wireless carrier, manufacturer and model, browser type, screen resolution, general location information such as city, state, or geographic area, and other device information collected automatically.</p>
I. Professional or Employment- Related Information	<p>Job application information, such as your resume or CV, background check information, references, and other information.</p> <p>Employment information, such as title, role, employer, employment history, current or past job history, and other professional information.</p>
J. Education Information	Education records , such as transcripts or education history.

K. Inferences Drawn from Personal Information	Profiles reflecting preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

We may collect the categories of personal information described above from the following sources:

- **Personal Information You Provide Us.** We collect the personal information that you provide to us while using our Platform, including contacting us, creating an account, applying for a position, or otherwise. Further, where expressly designated by MM, some portions of the Services may be used by active MM clients to communicate pursuant to an attorney/client relationship. You may choose whether or not to provide such information; however, the information may be required to respond to your request.
- **Personal Information Collected Automatically.** We and our third party providers may use cookies and other technologies such as log files, cookies, tracking pixels, and analytic tools and services to collect personal information automatically about you. Such information includes your geolocation and the online identifiers, device information, and online activity information described above. To facilitate the automatic collection described above, we may use the following technologies:
 - **Cookies.** A cookie is a small piece of data stored by your web browser on your computer or mobile device. We use cookies to collect information from you regarding your usage of the Platform in order to remember user preferences and settings, personalize your experience with the Platform, facilitate online advertising, and for security purposes. You may opt-out of the automatic collection of some information by referring to your web browser or mobile device options or settings menu. However, doing so may disable many of the portions, features, or functionality of the Platform. Each browser is different, so check the "Help" menu of your browser to learn how to change your cookie preferences or visit <http://www.allaboutcookies.org> for more information.
 - **Pixels.** Pixels, which are also known as "web beacons," or "clear GIFs," are typically used to determine whether a webpage or email was accessed or opened, or that certain content was viewed or clicked. Data collected from pixels is often used to compile statistics about usage of websites and the success of

email marketing campaigns.

- **SDKs.** Software development kits, or “SDKs,” are third-party computer codes used in connection with the App for a variety purposes, including to provide analytics regarding the use of the App, integrate with social media, add features or functionality to the App, or facilitate online advertising. SDKs may enable third parties to collect information directly via the App.
- **Personal Information Collected from Third Parties.** We may also collect or receive personal information from third parties, which may include:
 - **Our business partners,** such as third-party data providers and advertising partners.
 - **Public sources,** such as social media platforms and publicly-available records.
 - **Individuals or entities involved in our clients’ legal matters,** such as doctors, other parties, and other individuals that you may direct to provide us with information.
 - **Referral sources,** such as members of our referral network, website submissions, and other referral sources.

ONLINE ANALYTICS

We may use third party analytics tools, such as Google Analytics and Mouseflow, in order to better understand your use of our Platform and how we can improve them. These tools collect information sent by your browser or mobile device, including the pages you visit and other usage information. For more information regarding how Google collects, uses, and shares your information please visit

<http://www.google.com/policies/privacy/partners/>. For more information on Mouseflow’s privacy practices, please visit <https://mouseflow.com/privacy/>. To prevent data from being used by Google Analytics, you can download the opt-out browser add-on at: <http://tools.google.com/dlpage/gaoptout?hl=en>. You can opt out of Mouseflow analytics at: <https://mouseflow.com/opt-out/>.

USE OF PERSONAL INFORMATION

We may use the personal information we collect for the following purposes and as otherwise described in this Privacy Policy or at the time of collection:

- **To Provide Our Platform.** We use personal information to provide our services, including the Platform. For example, we use personal information:
 - to facilitate your requests for a free case evaluation

and determine your legal needs;

- to provide you with legal and other services, content, and features you request;
- to create, manage, and monitor your account;
- to respond to your inquiries and communicate with you, including placing calls or sending texts using any automated technology, including prerecorded messages;
- to operate, troubleshoot, and improve the Platform;
- to process your transactions, invoices, and settlement payments;
- to understand your interests, personalize your experience on the Platform, and deliver information about products and services relevant to your interests;
- respond to your inquiries and requests for customer support, including to investigate and address your concerns and monitor and improve our responses; and
- enable security features of the Platform, such as by sending you security codes via email or SMS, and remembering devices from which you have previously logged in.

- **For Direct Marketing.** We may use your personal information to send you newsletters, legal updates, event information, marketing communications, and other information that may interest you.
- **For Research and Development.** We use personal information for research and development purposes and to understand how people are using the Platform, including by generating and analyzing statistics, preferences, and usage trends, to make our Platform and other offerings better, diagnose technical issues, and develop new features and functionality. As part of these activities, we may create aggregated, de-identified or other anonymous data from personal information we collect. We make personal information into anonymous data by removing information that makes the data personally identifiable to you. We may use this anonymous data and share it with third parties for our lawful business purposes, including to analyze and improve the Platform and promote our business.
- **For Hiring Purposes.** If you apply to one of our open positions, submit application information or inquire about a position, we will use your personal information as part of the evaluation, recruitment, and hiring of personnel, including conducting background checks and contacting references.
- **For Compliance, Fraud Prevention and Safety.**
 - to enforce our Terms of Use and other agreements we may have;
 - to comply with applicable laws, regulations, and legal processes;

- to protect our, your, or others' rights, privacy, safety, or property (including by making and defending legal claims);
 - to maintain the security and integrity of our business, the Platform, users, our third party business partners and service providers our databases and other technology assets;
 - audit our internal processes for compliance with legal and contractual requirements and internal policies; and
 - prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks and identity theft.
- **For Interest-Based Advertising.** We, our business partners, and our third party advertising partners may collect and use your personal information for advertising purposes. We may contract with third-party advertising companies and social media companies to help us advertise our services, identify potential customers, and display ads on our Platform and other sites and services, including through the use of interest-based advertising. These companies may use cookies and similar technologies to collect information about you (including the device information and online activity information described above) over time across our Platform and other sites and services or your interaction with our emails, and use that information to serve ads that they think will interest you and/or use hashed customer lists that we share with them to deliver ads to you and to similar users on their sites and services. You can learn more about your choices for limiting interest-based advertising, in the "Advertising Choices" section below.

SHARING OF PERSONAL INFORMATION

In addition to the specific situations discussed elsewhere in this Privacy Policy or as otherwise described at the time of collection, we may share personal information with the following categories of recipients:

- **Service Providers.** MM may share your personal information with third-party service providers that perform services for us or on our behalf, such as web-hosting companies, mailing vendors, analytics providers, event hosting services, and information technology providers.
- **Other Law Firms or Lawyers.** MM may share, at your direction or with your permission, your personal information with other law firms and/or other lawyers where we jointly represent a client and when we refer cases or potential cases to other counsel, or as otherwise required in connection with our legal representation of you. Personal information provided pursuant to an

attorney/client relationship may not be shared with third parties except as is done with such precautions to preserve the confidentiality of such information and any attorney/client privilege as may attach to such information.

- **Authorities, Law Enforcement, and Others.** MM may disclose personal information to comply with laws, regulations or other legal obligations, to assist in an investigation, to protect and defend our rights and property, or the rights or safety of third parties, to enforce our agreements, Terms of Use or this Privacy Policy or agreements with third parties, or for crime-prevention purposes.
- **Business Transactions.** MM may disclose your personal information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a transaction (or potential transaction) such as a corporate divestiture, financing, merger, consolidation, acquisition, reorganization, sale, spin-off, or other disposition of all or any portion of the business or assets of, or equity interests in, MM or our related companies (including in connection with a bankruptcy or similar proceedings).
- **Advertising Partners.** We may share your personal information with third party advertising or joint marketing partners for the purposes described in this Privacy Policy or at the time of collection.
- **Professional Advisors.** We may disclose your personal information to our professional advisors, such as lawyers, bankers, auditors and insurers, where necessary in the course of the professional services that they render to us.
- **Affiliates and Related Companies.** We may share your personal information with companies that are affiliated with us (that is, that control, are controlled by, or are under common control with us) or may be affiliated with us in the future for the purposes described in this Privacy Policy.
- **Consent.** MM may otherwise disclose your Personal Information in accordance with your consent.

YOUR CHOICES

- **Opt-Out of Marketing Communications.** If you no longer wish to receive marketing communications from us, you can let us know by sending an email to contact@forthepeople.com or by mail at the address provided below in "Contact Us". The electronic marketing communications we send may also contain an opt-out mechanism. Please note that it may take up to 10 calendar days to remove your contact information from our marketing communications lists, so you may receive

correspondence from us for a short time after you make your request. Please also contact us to update or correct your information if it changes or if you believe that any information that we have collected about you is inaccurate.

- **Text Messages.** We may offer communications via SMS texts or similar technology sent by MM or our service providers, such as when we send you text messages for customer service, account-related, or marketing purposes. To stop receiving text messages from a short code operated by MM, reply STOP. Note that we may send you a message to confirm receipt of your STOP request. Message and data rates may apply for this service. You can also opt-out of

MM marketing texts by emailing us your request and mobile telephone number to contact@forthepeople.com.

- **Cookies.** Most browsers let you remove or stop accepting cookies from the websites you visit. To do this, follow the instructions in your browser's settings. Many browsers accept cookies by default until you change your settings. If you do not accept cookies, however, you may not be able to use all functionality of the Platform and our Site may not work properly. For more information about cookies, including how to see what cookies have been set on your browser and how to manage and delete them, visit www.allaboutcookies.org.
- **Advertising Choices.** Some of our advertising partners are members of the Network Advertising Initiative (NAI) and are subject to the Self-Regulatory Principles for Online Behavioral Advertising published by the Digital Advertising Alliance (DAA). You can obtain more information about these companies' information collection practices and opt-out of receiving interest-based advertising from participating NAI and DAA members at http://www.networkadvertising.org/managing/opt_out.asp and/or the DAA's website at optout.aboutads.info. You can also limit collection of your information for interest-based ads by blocking third party cookies in your browser settings or using privacy plug-ins or ad blocking software that help you block third party cookies. In addition, your mobile device settings may provide functionality to limit use of the advertising ID associated with your mobile device for targeted online advertising purposes. If you opt-out of interest-based advertisements, you will still see advertisements online but they may be less relevant to you. Some of the third party advertising companies we may work with offer their own opt-out options that you can use to limit their use of your information for interest-based advertising. Please note that we also may work with companies that offer their own opt-out mechanisms, such as Google (<https://adssettings.google.com/authenticated>) and Facebook (<https://www.facebook.com/about/ads>), or

do not participate in the opt-out mechanisms described above. Even after using these opt-out mechanisms, you may receive interest-based advertising from other companies.

- **Declining to Provide Information.** We need to collect personal information to provide certain services. If you do not provide the information requested, we may not be able to provide those services.

INFORMATION SECURITY

MM takes commercially reasonable measures to secure and protect the personal information we collect. Nevertheless, no security system is impenetrable. We cannot guarantee the absolute security of your personal information. Moreover, we are not responsible for the security of information you transmit to us over networks that we do not control, including the Internet and wireless networks.

LINKED WEBSITES

This Privacy Policy does not apply to third-party websites or social media features that may be accessed through links that we provide for your convenience and information. Accessing those links will cause you to leave MM's website and may result in the collection of information about you by a third party. We do not control, endorse or make any representations about those third party websites or their privacy practices, which may differ from ours. We encourage you to review the privacy policy of any site you interact with before allowing the collection and use of your information.

DO NOT TRACK REQUESTS

We adhere to the standards set out in this Privacy Policy and do not monitor or follow any Do Not Track browser requests. To find out more about "Do Not Track," please visit <http://www.allaboutdnt.com>.

USING THE PLATFORM FROM OUTSIDE THE UNITED STATES

MM is headquartered in the United States of America, and we may have affiliates and service providers in the United States and other countries. Please be aware that your personal information may be transferred to, stored or processed in the United States, where our servers are located and our central database is operated, and other locations outside of your home country. The

operated, and other locations outside of your home country. The data protection and other laws of these countries might not be as comprehensive as those in your country. By using any portion of the Platform, you understand and consent to the transfer of your personal information to our facilities in the United States and those third parties with whom we share it as described in this Privacy Policy.

CHILDREN'S PRIVACY

We do not knowingly solicit or collect personal information online from children under the age of 16. Please contact us as

provided below in the Contact Us section if you believe we may have collected such information.

YOUR CALIFORNIA PRIVACY RIGHTS

This section applies only to California residents. It describes how we collect, use, and share personal information of California residents when we act as a "business" as defined under California privacy law, and their rights with respect to their personal information. For purposes of this section, "personal information" has the meaning given under California privacy law but does not include information exempted from the scope of those laws. In some situations we may provide a different privacy notice to certain categories of California residents, whereby that notice will apply instead of this section.

California Civil Code Section § 1798.83 permits users of our Platform who are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to contact@forthepeople.com.

In addition, the state of California provides California residents with certain other rights concerning their personal information. This section describes (1) the categories of personal information, collected and disclosed by MM, subject to California privacy law, (2) your privacy rights under California privacy law, and (3) how to exercise your rights.

Personal Information That We Collect, Use, and Disclose

In accordance with California law, we describe:

- the categories of personal information we may have collected about you in the preceding 12 months and the categories of sources from which we collected your personal information in the section above called "Types of Personal Information We Collect";
- the business and commercial purposes for which we collect

this information in the section above called "Use of Personal Information"; and

- the categories of third parties to whom we disclose this information in the section above called "Sharing of Personal Information".

MM must also disclose whether the following categories of personal information are disclosed for a "business purpose" or "valuable consideration" as those terms are defined under California privacy law, which also calls this latter category a "sale." Note that while a category below may be marked, that does not necessarily mean that we have personal information in that category about you.

In the preceding twelve months, we have disclosed the following categories of personal information in the manner described:

Category	Personal Information is Disclosed for a Business Purpose	PurposePersonal Information is Disclosed for Valuable Consideration
A. Individual Identifiers and Demographic Information	Yes	Yes
B. Sensitive Personal Information	Yes	No
C. Geolocation Data	Yes	No
E. Sensory Data	Yes	No
F. Biometric Information	Yes	No
G. Commercial Information	Yes;	No

H. Internet or Network Activity	Yes	Yes
I. Professional or Employment-Related Information	Yes	No
J. Education Information	Yes	No
K. Inferences Drawn from Personal Information	Yes	No

Your Privacy Rights Under California Law

Under California law, subject to certain exceptions, California residents have the following rights with respect to their personal information:

- **Access.** You have the right to request information on the categories of personal information that we collected about you in the previous 12 months, the categories of sources from which the personal information was collected, the specific pieces of personal information we have collected about you, the business and commercial purposes for which such personal information is collected and shared, and the categories of third parties to whom we disclose such personal information.
- **Erasure.** You have the right to request we delete your personal information, subject to certain exceptions.
- **Opt-Out of Sales.** If we “sell” your personal information, you can opt-out.
- **Non-discrimination.** California residents are entitled to exercise the rights described above free from discrimination or legally prohibited increases in the price or decreases in the quality of our products and services.

Please note, these rights are not absolute and in some situations we may not be able to respond to your request, such as when a legal exemption applies or if we are not able to verify your identity.

How to Request to Exercise Your California Privacy Rights

If you would like to exercise your rights listed above, please follow the directions below:

- **Access and Erasure Rights.** Send (or have your authorized agent send) an email to contact@forthepeople.com or call us toll-free at: 1-(844) 256-4550.
- **Right to Opt-Out of the Sale of Personal Information.** Under California law, some of the personal information that we share with our advertising partners may qualify as a “sale” as defined under California privacy law. To exercise your right to opt-out of such “sale”, please:
 - Email us at contact@forthepeople.com, or
 - Click here: [Do Not Sell My Personal Information](#)

While we take measures to ensure that those responsible for receiving and responding to your request are informed of your rights and how to help you exercise those rights, when contacting us to exercise your rights, we ask you to please adhere to the following guidelines:

- **Tell Us Which Right You Are Exercising:** Specify which right you want to exercise and the personal information to which your request relates (if not to you). If you are an authorized agent acting on behalf of another consumer, please clearly indicate this fact and your authority to act on such consumer’s behalf. We may require the requester’s proof of identification, the authorized agent’s proof of identification, and any other information that we may request in order to verify your request, including evidence of valid permission to act on requester’s behalf.
- **Help Us Verify Your Identity:** Provide us with information to verify your identity. Please note that if we cannot initially verify your identity, we may request additional information to complete the verification process. Any personal information you disclose to us for purposes of verifying your identity will solely be used for the purpose of verification.
- **Direct Our Response Delivery:** Please provide us with an e-mail or mailing address through which we can provide our response. If you make the request by email, unless otherwise requested, we will assume that we can respond to the email address from which you made the request.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee or decline to comply with your request if your request is clearly unfounded, repetitive, or excessive.

We try to respond to all legitimate requests within 45 days of your request. Occasionally it may take us longer than 45 days to

respond, for instance if your request is particularly complex or you have made a number of requests. In this situation, we will notify you of the delay, and may continue to update you regarding the progress of our response.

CHANGES TO THIS PRIVACY POLICY

MM may change this Privacy Policy from time to time to reflect changes in our practices or in applicable law. Such changes will be effective upon posting the revised Privacy Policy on our Platform. You will be able to tell when this Privacy Policy was last updated by the Last Updated date included at the bottom of this

Privacy Policy. By continuing to use our Platform, or communicating electronically with us thereafter, you agree to accept such changes to this Privacy Policy.

CONTACT US

If you have any questions about this Privacy Policy or MM's information privacy practices, please contact us at:

E-mail: contact@forthepeople.com

Telephone: (407) 420-1414

Mail: Morgan & Morgan, PA, Attn: Privacy Policy, 20 North Orange Ave, Suite 1600, Orlando, FL 32801

LAST UPDATED: December 23, 2021

Quick Links

[Accessibility](#)
[Careers](#)
[Complaints](#)
[Referrals](#)
[Giving Back](#)
[Shop](#)
[Privacy Policy](#)
[Reviews](#)
[Terms & Conditions](#)
[Scholarships](#)
[Opt Out](#)

Trending News

[Everything You Need To Know About The Equifax Credit Score Glitch](#)
[Nintendo Threats Go Beyond Video Game Bad Guys – Old Hardware Poses Security Risks](#)
[JPMorgan Gold Traders Cheat Scam — Have You Been Spoofed?](#)

[Read more](#)

Most Asked Questions

[Why Morgan & Morgan?](#)
[What Damages Are Available in Mass Torts?](#)
[Why File a Mass Tort?](#)

[Read more](#)



Email address

Subscribe



© 2022. All Rights Reserved.

20 North Orange Ave, Suite 1600, Orlando, FL 32801 designed to be accessible to and usable by people with and without disabilities. Please contact us if you encounter an accessibility or usability issue on this site. Attorney advertising. Prior results do not guarantee a similar outcome. Do Not Sell My Personal Information

EXHIBIT 37

On Aug 6th 11 PM ET/Aug 7th 03:00 UTC, due to scheduled Firefox Account server maintenance, users may not be able to sign in or create a new subscription. This is expected to last approximately 30 minutes. Status updates can be found at <https://status.vpn.mozilla.org> or <https://status.relay.firefox.com>.

Support

moz://a



Protect your privacy

Customize this article

Download Firefox

[Systems and Languages](#) [What's New](#) [Privacy](#)



Common Myths about Private Browsing

[Private Browsing](#) is a useful feature of Firefox, but only if you understand the protection it offers. It helps you obscure your online activity from other people who use Firefox on your computer, but does not make you invisible online.

Myth 1: Private Browsing makes you anonymous on the Internet

Reality: Private Browsing does not mask your identity or activity online. Websites and [internet service providers can still gather information](#) about your visit, even if you are not signed in. If you use your device at work, your company may be able to monitor the websites you visit. If you surf the Web at home, your cable company (or their partners) may have access to your browsing information. Only a [Virtual Private Network](#) (VPN) can mask your location and encrypt your online activity, keeping your identity and data safe from prying eyes. If you need to stay anonymous online, try [Mozilla VPN](#).

Myth 2: Private Browsing removes all traces of your browsing activity from your computer

Reality: Private Browsing works by letting you browse without saving passwords, cookies and browsing history in a Private Window. If you download a file from a website, it will remain on your computer, but it will not appear in the download manager in Firefox. If you bookmark a website while in a Private Window, it will remain in your bookmark list.

Myth 3: Private Browsing doesn't display any browsing history

Reality: Private Browsing will, by default, [display visited sites and bookmarks as you type in the address bar](#). Firefox saves these pages during normal browsing. If you don't want to see these suggestions, you can deselect them in your Firefox Settings Privacy & Security panel under *Address Bar*.

Address Bar

When using the address bar, suggest

- ☐ Browsing history
- ☐ Bookmarks

Myth 4: Private Browsing will protect you from keystroke loggers and spyware

Reality: Private Browsing does not protect you from malware installed on your computer. If you suspect you have malware, [take steps to remove it](#) to prevent it from happening again.

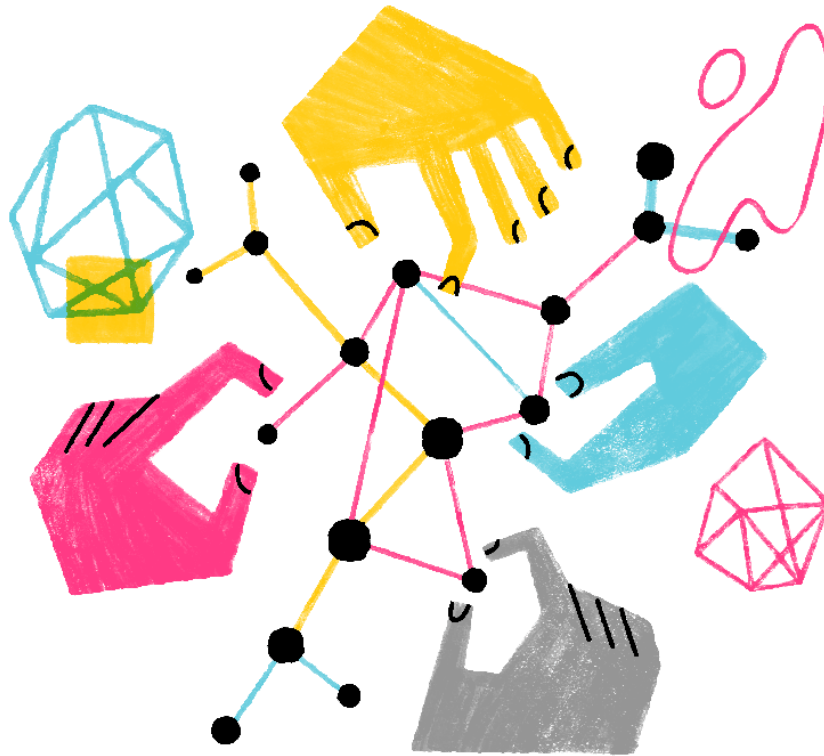
To learn more about how Firefox protects your privacy, see [Enhanced Tracking Protection in Firefox for desktop](#) and [SmartBlock for Enhanced Tracking Protection](#).

Was this article helpful?



These fine people helped write this article:

[AliceWyman](#), [Michele Rodaro](#), [Mozinet](#), [Joni](#), [Artist](#), [Jeff](#), [Erin S.](#), [Fabi](#), [k_alex](#), [Bithiah](#), [JeremyKoozar](#), [alineee](#)



Volunteer

Grow and share your expertise with others. Answer questions and improve our knowledge base.

[Learn More](#)

Mozilla

[Report Trademark Abuse](#)

[Source code](#)

[Twitter](#)

[Join our Community](#)

[Explore Help Articles](#)

Firefox

[Download](#)

[Firefox Desktop](#)

[Android Browser](#)

[iOS Browser](#)

[Focus Browser](#)

Firefox for Developers

[Developer Edition](#)

[Beta](#)

[Beta for Android](#)

[Nightly](#)

[Nightly for Android](#)

Firefox Accounts

[Sign In/Up](#)

[Benefits](#)

Firefox Private Network

Language [English](#)

[mozilla.org](#) [Terms of Service](#) [Privacy](#) [Cookies](#) [Contact](#)


Visit Mozilla Corporation's not-for-profit parent, the Mozilla Foundation.

Portions of this content are ©1998–2022 by individual mozilla.org contributors. Content available under a Creative Commons license.

EXHIBIT 38



Privacy, Microsoft Edge, Windows 10




The new Microsoft Edge  helps you browse, search, shop online, and more. Like all modern browsers, Microsoft Edge lets you collect and store specific data on your device, like cookies, and lets you send information to us, like browsing history, to make the experience as rich, fast, and personal as possible.

Whenever we collect data, we want to make sure it's the right choice for you. Some people worry about their web browsing history being collected. That's why we tell you what data is stored on your device or collected by us. We give you choices to control what data gets collected. For more information about privacy in Microsoft Edge, we recommend reviewing our [Privacy Statement](#).



What data is collected or stored, and why

Microsoft uses diagnostic data to improve our products and services. We use this data to better understand how our products are performing and where improvements need to be made.

Microsoft Edge collects a set of required diagnostic data to keep Microsoft Edge secure, up to date and performing as expected. Microsoft believes in and practices information collection minimization. We strive to gather only the info we need, and to store it only for as long as it's needed to provide a service or for analysis. In addition, you can control whether optional diagnostic data associated with your device is shared with Microsoft to solve product issues and help improve Microsoft products and services.

As you use features and services in Microsoft Edge, diagnostic data about how you use those features is sent to Microsoft. Microsoft Edge saves your browsing history—information about websites you visit—on your device. Depending on your settings, this browsing history is sent to Microsoft, which helps us find and fix problems and improve our products and services for all users. You can manage the collection of optional diagnostic data in the browser by selecting **Settings and more**  > **Settings**  > **Privacy, search, and services**  and turning on or off **Help improve Microsoft products by sending optional diagnostic data about how you use the browser, websites you visit, and crash reports**. This includes data from testing new experiences. To finish making changes to this setting, restart Microsoft Edge.

Turning this setting on allows this optional diagnostic data to be shared with Microsoft from other applications using Microsoft Edge, such as a video streaming app that hosts the Microsoft Edge web platform to stream the video. The Microsoft Edge web platform will send info about how you use the web platform and sites you visit in the application to Microsoft. This data collection is determined by your optional diagnostic data setting in Privacy, search, and services settings in Microsoft Edge.

On Windows 10, these settings are determined by your Windows diagnostic setting. To change your diagnostic data setting, select **Start**  > **Settings**  > **Privacy**  > **Diagnostics & feedback** . On all

other platforms, you can change your settings in Microsoft Edge by selecting **Settings and more** ⋮

> **Settings** ⚙️ > **Privacy, search, and services** 🛡️. In some cases, your diagnostic data settings might be managed by your organization.

When you're searching for something, Microsoft Edge can give suggestions about what you're searching for.

To turn on this feature, select **Settings and more** ⋮ > **Settings** ⚙️ > **Privacy, search, and services** 🛡️

> **Address bar and search**, and turn on **Show me search and site suggestions using my typed characters**. As you start to type, the info you enter in the address bar is sent to your default search provider to give you immediate search and website suggestions.

When you use InPrivate browsing or guest mode, Microsoft Edge collects some info about how you use the browser depending on your Windows diagnostic data setting or Microsoft Edge privacy settings, but automatic suggestions are turned off and info about websites you visit is not collected. Microsoft Edge will delete your browsing history, cookies, and site data, as well as passwords, addresses, and form data when you close all InPrivate windows. You can start a new InPrivate session by selecting **Settings and more** on a computer or **Tabs** on a mobile device.

Microsoft Edge also has features to help you and your content stay safe online. Windows Defender SmartScreen automatically blocks websites and content downloads that are reported to be malicious. Windows Defender SmartScreen checks the address of the webpage you're visiting against a list of webpage addresses stored on your device that Microsoft believes to be legitimate. Addresses that aren't on your device's list and the addresses of files you're downloading will be sent to Microsoft and checked against a frequently updated list of webpages and downloads that have been reported to Microsoft as unsafe or suspicious.

To speed up tedious tasks like filling out forms and entering passwords, Microsoft Edge can save info to help. If you choose to use those features, Microsoft Edge stores the info on your device. If you've turned on sync for form fill like addresses or passwords, this info will be sent to the Microsoft cloud and stored with your Microsoft account to be synced across all your signed-in versions of Microsoft Edge. You can manage this data from **Settings and more** ⋮ > **Settings** ⚙️ > **Profiles** 👤.

To protect some video and music content from being copied, some streaming websites store Digital Rights Management (DRM) data on your device, including a unique identifier (ID) and media licenses. When you go to one of these websites, it retrieves the DRM info to make sure you have permission to use the content.

Microsoft Edge also stores cookies, small files that are put on your device as you browse the web. Many websites use cookies to store info about your preferences and settings, like saving the items in your shopping cart so you don't have to add them each time you visit. Some websites also use cookies to collect info about your online activity to show you interest-based advertising. Microsoft Edge gives you options to clear cookies and block websites from saving cookies in the future.

Microsoft Edge will send Do Not Track requests to websites when the **Send Do Not Track requests** setting is turned on. Websites may still track your activities even when a Do Not Track request is sent, however.

How to clear data collected or stored by Microsoft Edge





To clear browsing info stored on your device, like saved passwords or cookies:

1. In Microsoft Edge, select **Settings and more** ⋮ > **Settings** ⚙️ > **Privacy, search, and services** 🛡️.
2. Under **Clear browsing data**, select **Choose what to clear**.





3. Under **Time range**, choose a time range.
4. Select the check box next to each data type you'd like to clear, and then select **Clear now**.
5. If you'd like, you can select **Choose what to clear every time you close the browser** and choose which data types should be cleared.

[Learn more about what gets deleted for each browser history item.](#)




To clear browsing history collected by Microsoft:



- To see your browsing history associated with your account, sign in to your account at account.microsoft.com. In addition, you also have the option of clearing your browsing data that Microsoft has collected using the [Microsoft privacy dashboard](#).
- To delete your browsing history and other diagnostic data associated with your Windows 10 device, select **Start**  > **Settings**  > **Privacy**  > **Diagnostics & feedback** , and then select **Delete** under **Delete diagnostic data**.





To clear individual passwords stored by Microsoft Edge on your device:

1. In Microsoft Edge, select **Settings and more**  > **Settings**  > **Profiles** , and then select **Passwords**.
2. Under **Saved passwords**, select **More actions**  next to a website name, and then select **Delete** to clear the password saved for that site.

How to manage your privacy settings in Microsoft Edge

To change your level of tracking prevention, clear your browsing data, help improve Microsoft Edge, and more, select **Settings and more**  > **Settings**  > **Privacy, search, and services** .

To choose if websites can ask for permission to use your location, camera, microphone, and more, select **Settings and more**  > **Settings**  > **Site permissions**.

To choose what types of data are synced across your devices, or to turn off syncing entirely, select **Settings and more**  > **Settings**  > **Profiles**  > **Sync** .

To learn more about privacy in Microsoft Edge, read the [Microsoft Edge privacy whitepaper](#).



 [SUBSCRIBE RSS FEEDS](#)

Need more help?

How can we help you?



Join the discussion

[ASK THE COMMUNITY >](#)

Get support

[CONTACT US >](#)

Was this information helpful?

Yes

No

What's new

Surface Laptop Go 2

Surface Pro 8

Surface Laptop Studio

Surface Pro X

Surface Go 3

Surface Duo 2

Surface Pro 7+

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store
support

Returns

Order tracking

Virtual workshops and
trainingMicrosoft Store
Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for
EducationMicrosoft 365
EducationEducation consultation
appointmentEducator training and
developmentDeals for students and
parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft Industry

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech
Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability



English (United States)

[Sitemap](#)[Contact Microsoft](#)[Privacy](#)[Terms of use](#)[Trademarks](#)[Safety & eco](#)[About our ads](#)[© Microsoft 2022](#)

EXHIBIT 39



Microsoft support
 Microsoft 365
 Office
 Windows
 Surface
 Xbox
 Deals

Microsoft Edge support

Products ▾

Devices

Search 🔍

Import favorites

Buy Microsoft 365


Sign in

Browse InPrivate

Add extensions

Microsoft Edge, Windows 11, Microsoft account dashboard

More support ▾

The new Microsoft Edge  will delete your browsing history, cookies, and site data, as well as passwords, addresses, and form data when you close all InPrivate windows.

You can open an InPrivate window in different ways:

- Select and hold (right-click) the Microsoft Edge logo in the taskbar and select **New InPrivate window**.
- In Microsoft Edge, select and hold (right-click) a link and select **Open link in InPrivate window**.
- In Microsoft Edge, select **Settings and more** '...' > **New InPrivate window**.

Other people using this device won't see your browsing activity, but your school, workplace, and internet service provider might still be able to access this data.

What does Microsoft Edge do with your data while InPrivate?





InPrivate browsing:

- Clears browsing history, download history, cookies and other site data, cached images and files, passwords, autofill form data, site permissions and hosted app data when you close all InPrivate windows.
- Saves your favorites and downloaded files, so you can access them next time you use Microsoft Edge.
- Allows you to access favorites, passwords, and form fill data from the profile used to open the InPrivate window.
- Allows extensions you've given permission to run while browsing InPrivate.
- Automatically uses InPrivate search with Microsoft Bing:
 - For searches in the InPrivate landing page search bar.
 - On Bing.com.
 - In the address bar, if Microsoft Bing is the default search engine.

Notes:



- Microsoft services may approximate your general area to provide relevant experiences like weather and news. Your location may be approximated using technologies like Bluetooth, WiFi, cellular modem, and IP address, or via the Windows location service if you have enabled location settings on your Windows device. Your general location data is cleared from the browser when you close all InPrivate windows.
- Microsoft Edge can't prevent extensions from saving your browsing history while browsing InPrivate.
- When using the Windows IME keyboard for typing and inking, data may be collected to improve language recognition and suggestion capabilities. To stop inking and typing data from being collected by Microsoft while using the Windows IME keyboard in InPrivate and normal browsing windows, go to **Windows Settings > Privacy & security > Inking & typing personalization**.
- Webpages such as <edge://settings>, <edge://favorites>, and <edge://history> can't be viewed in an InPrivate window. Opening these pages when browsing InPrivate will open them in a normal browsing window.

InPrivate browsing does not:

- Prevent websites from requesting your precise location. InPrivate browsing uses the location permission settings of the profile from which the InPrivate session was launched. To manage location permissions, go to **Settings and more**  **Settings**  **Cookies and site permissions > Location**.
- Associate your browsing history with a Microsoft account or use this data for product improvement.
- Save new passwords, addresses, or information filled in online forms.
- Allow you to re-open recently closed tabs and windows from **Settings and more**  **History**  **Recently closed**.

Am I safer while browsing InPrivate?

InPrivate browsing doesn't keep you safer from malicious websites or provide additional ad blocking. Websites can still personalize content for you during your InPrivate browsing session because cookies and other site permissions aren't deleted until you close all InPrivate windows.

To help prevent websites from personalizing content and ads for you, [switch your level of tracking prevention to Strict in Microsoft Edge](#) or go to **Settings and more**  **Settings**  **Cookies and site permissions > Manage and delete cookies and site data** and turn on **Block third-party cookies**. This might cause some sites to behave unexpectedly.

When is InPrivate browsing unavailable?

Children with activity reporting or web filtering enabled through their family group can't browse InPrivate. Organizations, like schools or workplaces, can use group policy to prevent people from browsing InPrivate.



Need more help?

How can we help you?



Join the discussion

[ASK THE COMMUNITY >](#)

Get support

[CONTACT US >](#)

Was this information helpful?

Yes

No

What's new

Surface Laptop Go 2

Surface Pro 8

Surface Laptop Studio

Surface Pro X

Surface Go 3

Surface Duo 2

Surface Pro 7+

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store
support

Returns

Order tracking

Virtual workshops and
trainingMicrosoft Store
Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for
EducationMicrosoft 365
EducationEducation consultation
appointmentEducator training and
developmentDeals for students and
parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft Industry

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech
Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability



English (United States)

[Sitemap](#)[Contact Microsoft](#)[Privacy](#)[Terms of use](#)[Trademarks](#)[Safety & eco](#)[About our ads](#)[© Microsoft 2022](#)